

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

JESSICA KERR, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

**CELSIUS NETWORK INC., CELSIUS
NETWORK LLC, and CELSIUS
LENDING LLC,**

Defendants.

Case No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

1. Plaintiff Jessica Kerr (“Kerr” or “Plaintiff”), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against defendants Celsius Network Inc., Celsius Network LLC, and Celsius Lending LLC (collectively “Celsius” or “Defendants”).

2. Plaintiff brings this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding individuals’ sensitive personal data—specifically their email addresses and home addresses (collectively known as “Private Information”).

3. As part of Celsius’ Chapter 11 bankruptcy proceedings, Celsius posted, unredacted, on the court’s public docket private information for over a half a million of its customers, including customer names, account holdings, transaction details, and the balances of their accounts. (the “Data Breach”). As a result, the Private Information of thousands of individuals was compromised.

5. Many members of the putative Class have already noted a marked increase in spam phone calls, spam emails, and other indications of fraudulent activity. As a result of Defendants’ breaches of duty and negligence, Celsius violated Plaintiff’s and the Class’ privacy

and posted the confidential data on the public docket. As a result, Defendants sent emails to customers instructing them to engage in monitoring of their accounts and electronic records and communications for phishing scam emails purporting to be Celsius. Samples of those email communications are annexed as Exhibit A hereto and incorporated by reference herein.

Defendants' negligence and breaches of duty have caused Plaintiff Kerr to be the victim of major fraudulent activity, described below.

6. Defendants' incompetent filing enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach as instructed by Celsius, including, as appropriate, reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

7. The Data Breach was caused by Defendants' violation of their obligations to exercise sufficient care in protecting customer information. Defendants' own motion requesting permission to file these documents without the very information that Defendant negligently included indicates that Defendants were fully aware of the risks inherent in divulging all of this information.

8. Accordingly, Plaintiff asserts claims for negligence, Violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201 et seq., and breach of confidence.

9. Plaintiff also seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF JESSICA KERR

10. Plaintiff Jessica Kerr is a resident and citizen of Florida and brings this action in her individual capacity and on behalf of all others similarly situated.

11. Plaintiff Kerr was a crypto-currency account holder with Celsius.

12. In maintaining Plaintiff Kerr's Private Information, Defendants expressly and impliedly promised to safeguard it. Defendant, however, did not act with necessary care and prudence to safeguard client data, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

13. On or around October 27, 2022, Plaintiff Kerr received phishing emails that she believed were sent from Celsius. Plaintiff Kerr was scammed by these emails resulting in a loss in the amount of \$3,500.

14. Plaintiff and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendants' ineffective data security measures, as further set forth herein.

15. Plaintiff Kerr greatly values her privacy and was distressed to learn that Defendants had negligently filed her Private Information and allowed cybercriminals to access said information.

B. DEFENDANTS

16. Defendant Celsius Network Inc. is a Delaware corporation with its principal place of business at 50 Harrison St, Suite 209F, Hoboken, NJ 07030.

17. Defendant Celsius Network LLC is a Delaware corporation with its principal place of business at 50 Harrison St, Suite 209F, Hoboken, NJ 07030.

18. Defendant Celsius Lending LLC is a Delaware corporation with its principal place of business at 50 Harrison St, Suite 209F, Hoboken, NJ 07030.

19. Defendants provided cryptocurrency investing services nationwide.

20. Clients routinely provided Defendants with their Private Information as part of receiving Defendants' services.

JURISDICTION AND VENUE

21. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

22. The Court has personal jurisdiction over Defendant Celsius Network Inc. because its principal place of business is located, and it conducts substantial business, in this District. The Court has personal jurisdiction over Defendant Celsius Network LLC because its principal place of business is located, and it conducts substantial business, in this District.

23. The Court has personal jurisdiction over Defendant Celsius Lending LLC because its principal place of business is located, and it conducts substantial business, in this District. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants are each incorporated in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTUAL ALLEGATIONS

24. Plaintiff's and Class members' Private Information was collected by Defendants through Defendants' regular business operations. As part of its bankruptcy proceedings, Celsius was required to disclose demographic information about its clients. On September 28, 2022, in response to a motion by Celsius, the Southern District of New York Bankruptcy Court issued a Memorandum Opinion and Order authorizing Celsius to redact the email addresses and home addresses of clients.

25. In this order, the court found a high likelihood that revealing clients' email addresses and home addresses would create an unjustifiable risk of fraud:

The Court further finds that there is cause under Section 107(c) of the Bankruptcy Code to protect individual account holders' personally identifying information, but only with respect to email and physical addresses. Such information, in combination with their names, could make individual account holders more vulnerable to identify theft and render account holders' crypto assets more susceptible to criminal theft. (Committee Joinder ¶ 6; see also ECF Doc. # 633 ¶ 2 (stating that "public disclosure of customers' email addresses . . . would put customer accounts at greater risk from hackers. It would also make customers all-too-easy targets for identity theft, phishing attacks and other scams."); ECF Doc. # 642 ¶ 2 ("[P]ublishing the contact information consisting of home addresses and email addresses of the Debtors' customers publicly on the docket . . . puts individuals at risk of identity theft, fraud or other serious harm.").)

In re Celsius Network LLC, ECF Doc. # 910, No. 1:22bk10964.

26. On or about October 5, 2022, Defendants uploaded entirely *unredacted* client information to the court's public docket. Defendants thereafter noticed the error and removed the unredacted information several hours later.

27. However, in this time, malicious parties were able to gain access to this data and take advantage of the information that was released.

28. This data contains sensitive information relating to over 600,000 individuals.

29. The Data Breach was described by industry experts as "one of the worst exchange data breaches[.]"¹ Furthermore, experts maintained that the breach exposed "Celsius users to exploitation by any rip-off artist or thief who combs through the data, connects it to other

¹ <https://www.wired.com/story/celsius-user-data-dump-crypto-tracing-scammers/> (last visited August 2, 2024).

accounts, and identifies their crypto currency holdings as a ripe target.”² That is exactly what took place here. As a result Plaintiff and Class members have been targets of cyber thieves and have suffered theft and fraud dues to Defendants’ reckless acts.

30. The Data Breach occurred because Celsius failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendants failed to competently undertake docket filings.

31. Defendants disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members’ Private Information was safeguarded, failing to take available steps to prevent an unintentional disclosure of data. As a result, the Private Information of Plaintiffs and Class members was unintentionally exposed to access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiff and Class members have a continuing interest in ensuring that their compromised Information is and remains safe.

A. Defendants Failed to Comply with Industry Standards and Federal and State Law

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members’ Private Information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members’ Private Information from disclosure.

33. Defendants had obligations created by industry standards and federal and state law to keep Class members’ Private Information confidential and to protect it from unauthorized access and disclosure.

34. Charged with handling sensitive Private Information, Defendants knew, or should have known, the importance of safeguarding parties’ Private Information that was entrusted to it

² *Id.*

and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on consumers after a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

35. Defendants' wanton recklessness in handling client information ignored "basic best practices" for docket and file management. These best practices were known, or should have been known, by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information. Even if they were ignorant about these "best practices" the Court's own direction to Defendants' instructed them to redact the information.

36. Defendants apparently did not follow these precautions because they regularly uploaded the wrong files to the court's public docket.

37. The potential for improper disclosure of Plaintiff and Class members' Private Information was a known risk to Defendant, and thus Defendants was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

B. Defendants Exposed Plaintiff and Class Members to Identify Theft, Financial Loss, and Other Harms

38. Plaintiff and Class members have been injured by the disclosure of their Private Information in the Data Breach.

39. The fact that Plaintiff and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

40. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.³ Indeed, a robust "cyber black market" exists in which

³ Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>.

criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

41. The value of Plaintiff and Class members' Private Information on the black market is substantial. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was \$1,349.⁴

42. The FTC has also recognized that consumer data is a valuable form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

*“Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.”*⁵

43. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.⁶ The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

44. The ramifications of Defendants' failure to keep parties' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that

⁴ See U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), <https://www.bjs.gov/content/pub/pdf/vit14.pdf> [hereinafter *Victims of Identity Theft*].

⁵ *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

⁶ *Web's Hot New Commodity*, *supra* note 17.

information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

45. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

46. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about an individual that can be logically associated with other information can be chained together, increasing its utility to criminals.

47. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the “mosaic effect.”

48. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users’ names.

C. Plaintiff and Class Members Suffered Damages from the Data Breach

49. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

50. The ramifications of Defendants’ failure to keep Class Members’ Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.⁷

51. In addition to its obligations under state and federal laws and regulations, Defendants owed a common law duty to Plaintiff and Class members to protect the Private

⁷ 2014 LexisNexis *True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>.

Information that is held, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

52. Defendants further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

53. As a direct result of Defendants' intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

54. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

55. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiff and other Class members' lives. Each Plaintiff received a cryptically written notice email from Defendants stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Information could have gone, or who might have access to it.

56. Plaintiff and the Class face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulently in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class

members may already be victims of identity theft and fraud without realizing it.

57. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

58. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

59. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves.

60. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

61. The Private Information belonging to Plaintiff and Class members is private and was left ineptly handled by Defendants who did not obtain Plaintiff or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

62. The Data Breach was a direct and proximate result of Defendants' failure to competently handle sensitive client information.

63. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

64. The U.S. Department of Justice's Bureau of Justice Statistics found that "among

victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems” and that “resolving the problems caused by identity theft [could] take more than a year for some victims.”⁸

65. Defendants did not take any measures to assist Plaintiff and Class members.

66. Defendants’ failure to adequately protect Plaintiff and Class members’ Private Information has resulted in Plaintiff and Class members being required to undertake numerous tasks to protect their identities, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while Defendants sits by and does nothing to assist those affected by the incident. Instead, as Defendants’ notice confirms, the burden is on Plaintiff and Class members to discover possible fraudulent activity and identity theft and mitigate the negative impacts arising from such fraudulent activity on their own.

67. Plaintiff Kerr has spent at least twenty-four (24) hours to date in conformance with Defendants’ instructions to monitor accounts. Spending at least an hour each month, checking her accounts for fraudulent activity, since the occurrence of the breach.

68. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

⁸ See U.S. Dep’t of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), <https://www.bjs.gov/content/pub/pdf/vit14.pdf> [hereinafter *Victims of Identity Theft*].

69. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

70. Plaintiff was a victim of such misuse of her information as a result of Defendants' negligence and breaches.

71. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further

breaches so long as Defendants fails to undertake appropriate measures to protect the Private Information in its possession;

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and
- Anxiety and distress resulting from fear of misuse of their Private Information.

72. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

73. Plaintiffs brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a “Nationwide Class” and a “Florida Subclass” (collectively, the “Class”) defined as:

Nationwide Class

All Celsius customers whose Private Information was publicly disclosed by Defendants in October of 2022.

Florida Subclass

All Celsius customers who are citizens of Florida whose Private Information was publicly disclosed by Defendants in October of 2022.

74. Excluded from both the Nationwide Class and the Florida Subclass (collectively defined as the “Class”) are Defendants and Defendants’ affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

75. Certification of Plaintiff’s claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

76. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class has thousands of members.

77. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, inter alia:

- a. Whether Defendants’ data management procedures prior to the Data Breach complied with applicable data security laws and regulations including, e.g., FTCA and the FDUPTA (as discussed below);
- b. Whether Defendants’ data security management practices prior to and during the Data Breach were consistent with industry standards;
- c. Whether Defendants improperly implemented their purported security practices to protect Plaintiffs’ and the Class’s Private Information from unauthorized capture, dissemination, and misuse;
- d. Whether Defendants failed to take reasonable measures to determine the extent of the Data Breach after they first learned of same;
- e. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff’s and the Class’s Private Information;

- f. Whether Defendants was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- g. Whether Defendants was unjustly enriched by its actions; and
- h. Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

78. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

79. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiff.

80. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class he seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

81. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendants has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

82. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class are relatively small

compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

**(On Behalf of the Nationwide Class, or,
Alternatively, the Florida Subclass)**

83. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

84. Upon Defendants' accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

85. Defendants owed a duty of care not to subject Plaintiff's and Class members' Private Information to an unreasonable risk of exposure and theft because Plaintiff and Class members were foreseeable and probable victims of any inadequate security practices.

86. Defendants owed numerous duties to Plaintiff and the Class, including the following:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- b. to protect Private Information using reasonable and adequate security

procedures and systems that are compliant with industry-standard practices;
and

- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

87. Defendants breached their duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard file and docket management principles, despite obvious risks, by ineptly disclosing clients' Private Information. Furthering its dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse it and intentionally disclose it to others without consent.

88. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the cryptocurrency industry.

89. Defendants knew, or should have known, that its data management practices did not adequately safeguard Plaintiff's and Class members' Private Information.

90. Defendants were in a position to ensure that its processes were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

91. Defendants breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

92. Because Defendants knew that a breach of client information would damage thousands of parties, including Plaintiff and Class members, Defendants had a duty to adequately maintain client information.

93. Defendants' duty of care to use reasonable security measures arose from of the special relationship that existed between Defendants and its parties, which is recognized by data

privacy laws and regulations under the laws of 13 states.

94. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

95. Defendants’ duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

96. Defendants’ own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendants’ misconduct included failing to: (1) secure Plaintiffs’ and Class members’ Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

97. Defendants breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members’ Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members’ Private Information;
- b. Failing to adequately monitor the security of Defendants’ networks and systems;
- c. Allowing unauthorized access to Class members’ Private Information;
- d. Failing to detect in a timely manner that Class members’ Private Information had been compromised; and
- e. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

98. Through Defendants' acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendants' possession or control.

99. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

100. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

101. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

102. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II

Violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA")

Fla. Stat. § 501.201 *et seq.*

(On Behalf of Plaintiff and the Florida Subclass)

103. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

104. Plaintiff, Class Members, and Defendants each qualify as a person engaged in trade or commerce as contemplated by the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201, *et seq.*

105. As alleged herein in this Complaint, Defendants engaged in unfair or deceptive

acts or practices in the conduct of consumer transactions in violation of FDUTPA, including but not limited to:

- a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;
- c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

106. Defendants' representations and omissions were material because they were likely to deceive reasonable account holders about the adequacy of Defendants' data security and

ability to protect the confidentiality of employees' Private Information.

107. In addition, Defendants' failure to secure creditors' PII violated the FTCA, and therefore violated the FDUTPA.

108. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard the Personal Information of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

109. The aforesaid conduct constitutes a violation of FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce.

110. The Defendants' violations of FDUTPA have an impact of great and general importance on the public, including Floridians. Defendants hold the Personal Information of numerous Floridians, many of whom have been impacted by the Data Breach. In addition, Florida residents have a strong interest in regulating the conduct of corporations such as Defendant, whose policies and practices described herein affected thousands across the country.

111. As a direct and proximate result of Defendants' violation of FDUTPA, Plaintiff and Class Members are entitled to judgment under Fla. Stat. § 501.201, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

112. Defendants' implied and express representations that it would adequately safeguard Plaintiff's and other Class Members' Private Information constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Fla. Stat. § 501.202(2).

113. On information and belief, Defendants formulated and conceived of the systems it used to compile and maintain employee information largely within the state of Florida, oversaw its data privacy program complained of herein from Florida, and its communications and other efforts to hold employee data largely emanated from Florida.

114. Defendants' implied and express representations that it would adequately

safeguard Plaintiffs' and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204.

115. Defendants knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendants advertised it is committed to protecting privacy and securely maintaining personal information. Defendants did not securely maintain personal information as represented, in violation of Fla. Stat. § 501.171.

116. These violations have caused financial injury to Plaintiff and Class Members and have created an unreasonable, imminent risk of future injury.

117. Accordingly, Plaintiff, on behalf of herself and the other Class Members, bring this action under the Florida Deceptive and Unfair Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT III
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class or, Alternatively, the Florida Subclass)

118. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

119. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendants and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

120. Defendant, in taking possession of this highly sensitive information, has a special relationship with affected parties, including Plaintiff and the Class. As a result of that special relationship, Defendants was provided with and stored private and valuable information

belonging to Plaintiff and the Class, which Defendants was required by law and industry standards to maintain in confidence.

121. Plaintiff and the Class provided such Private Information to Defendants under both the express and/or implied agreement of Defendants to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiff's and Class members' consent.

122. Defendants had a common law duty to maintain the confidentiality of Plaintiffs' and Class members' Private Information.

123. Defendants owed a duty to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

124. As a result of the parties' relationship of trust, Defendants had possession and knowledge of the confidential Private Information of Plaintiff and Class members.

125. Plaintiff's and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class members did not consent to nor authorize Defendants to release or disclose their Private Information to unknown criminal actors.

126. Defendants breached the duty of confidence it owed to Plaintiff and Class members when Plaintiff's and Class members' Private Information was disclosed to unknown criminal hackers by way of Defendants' own acts and omissions, as alleged herein.

127. Defendants knowingly breached its duties of confidence by failing to safeguard Plaintiff's and Class members' Private Information, including by, among other things:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test

and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiffs and Class members thereof; (g) failing to follow its own privacy policies and practices published to consumers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

128. But for Defendants' wrongful breach of confidence owed to Plaintiff and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

129. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to

undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their confidential Private Information.

130. Defendants breached the confidence of Plaintiff and Class members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendants to retain the benefits it has received at Plaintiffs' and Class members' expense.

131. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT IV
INJUNCTIVE RELIEF

132. **(On Behalf of the Nationwide Class or, Alternatively, the Florida Subclass)**

133. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

134. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

135. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective duties to reasonably safeguard users' Private Information and whether Defendants is maintaining data security measures adequate to protect the Class members, including Plaintiff, from further data breaches that compromise their Private Information.

136. Plaintiff alleges that Defendants' data-security measures remain inadequate. In addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their

Private Information and remain at imminent risk that further compromises of their Private Information and fraudulent activity against them will occur in the future.

137. Pursuant to its authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) Defendants owe a duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law and various federal and state statutes; and (ii) Defendants are in breach of these legal duties by failing to employ reasonable measures to secure consumers' Private Information in its possession and control.

138. Plaintiff further ask the Court to issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information from future data breaches.

139. If an injunction is not issued, the Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, the Class members will not have an adequate remedy at law because many of the resulting injuries would not be readily quantifiable and Class members will be forced to bring multiple lawsuits to rectify the same misconduct.

140. The hardship to the Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendants, the Class members will likely be subjected to substantial hacking and phishing attempts, fraud, and other instances of the misuse of their Private Information, in addition to the damages already suffered. On the other hand, the cost to Defendants of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendants has pre-existing legal obligations to employ such measures.

141. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at

Defendant, thus eliminating the additional injuries that would result to the Class members and the consumers whose personal and confidential information would be further compromised.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class or, Alternatively, the Florida Subclass)

142. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

143. In providing their Private Information to Defendants, Plaintiff and Class members justifiably placed a special confidence in Defendants to act in good faith and with due regard for the interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

144. Defendants accepted the special confidence Plaintiff and Class members placed in them.

145. In light of the special relationship between Defendants and Plaintiff and Class members, whereby Defendants became a guardian of Plaintiff and Class members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class members for the safeguarding of Plaintiff and Class members' Private Information.

146. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers.

147. Defendants breached its fiduciary duties to Plaintiff and Class members by failing to protect the confidentiality of Plaintiff and Class members' Private Information.

148. Defendants breached their fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff and Class members' Private Information.

149. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of the services they paid for and received.

150. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- a. For an order certifying the proposed classes and appointing Plaintiff and their counsel to represent the Class;
- b. For an order awarding Plaintiff and Class members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;


- c. For an order awarding Plaintiff and Class members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;
- d. For an order or orders requiring Defendants to adequately remediate the Breach and its effects.
- e. For an order awarding Plaintiff and Class members pre-judgment and post-judgment interest;
- f. For an order awarding Plaintiff and Class members compensatory damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;
- g. For an order awarding Plaintiff and the Class members reasonable attorneys' fees and costs of suit, including expert witness fees;
- h. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury on all claims so triable.

Dated: November 4, 2024

By:



Gary S. Graifman, Esq.
**KANTROWITZ, GOLDHAMER &
GRAIFMAN, P.C.**
135 Chestnut Ridge Road, Suite 200
Montvale, New Jersey 07645
Tel: 201-391-7000
Fax: 201-307-1086
ggraifman@kgglaw.com

Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com

Jason S. Rathod*

jrathod@classlawdc.com

MIGLIACCIO & RATHOD LLP

412 H Street NE, no. 302,

Washington, DC, 20002

Office: (202) 470-3520

Scott D. Hirsch, Esq.*

scott@scotthirschlawgroup.com

SCOTT HIRSH LAW GROUP PLLC

6810 N. State Road 7,

Coconut Creek, FL 33073

Office: (561) 569-6283

* *pro hac vice* forthcoming

*Attorneys for Plaintiff and the Proposed
Class*